
Seattle Police Department

Information Systems, Processes, Operations and Technologies

Current State and Maturity Analysis

Current State

December 2013

Version: Final

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

Document revision list

Version	Date	Change Description
Draft 1.0	9/3/2013	Initial Draft
Draft 1.1	9/16/2013	Updated Draft
Draft 1.2	9/26/2013	Updated Draft
Draft 1.3	10/3/2013	Updated Draft
Draft 1.4	10/15/2013	Updated Draft
Draft 1.5	10/19/2013	Updated Draft
Draft 2.0	10/20/2013	Content revisions
Draft 3.0	10/21/2013	Content revisions
Draft 4.0	10/22/2013	Content revisions
Draft 5.0	10/22/2013	Content revisions
Draft 5.1	10/23/2013	Content revisions
Draft 6.0	10/23/2013	Content revisions
Draft 6.1	10/24/2013	Content revisions
Draft 7.0	11/6/2013	Revised content based on feedback
Draft 7.1	11/10/2013	Content revisions
Draft 7.2	11/11/2013	Content revisions
Final	12/6/2013	Final Version

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

Contents

1.	<i>Executive Summary</i>	6
1.1.	Introduction	6
1.2.	Objective	6
1.3.	Journey to Date	7
1.4.	Methodology	8
1.5.	Scope	10
1.6.	Findings	13
2.	<i>Current State IT Analysis</i>	15
2.1.	Overview of SPD IT	15
2.2.	Notes on Current State Analysis	17
2.3.	Technology	17
2.3.1.	Single Sign On (SSO)	17
2.3.2.	Data Management	18
2.3.3.	Content & Document Management	20
2.3.4.	Integration	21
2.3.5.	Development Platform	22
2.3.6.	Overall Technology related findings	23
2.4.	Resources	25
2.4.2.	Overall Resource related findings	26
2.5.	Processes	27
2.5.1.	Project Management	27
2.5.2.	Configuration Management/Change Management/Release Management/Event Management	28
2.5.3.	IT Governance	29
2.5.4.	Development Standards	30
2.5.5.	Testing Standards	31
2.5.6.	Security	31
2.6.	Systems	32
2.6.1.	PEDS	32
2.6.2.	AIM	35
2.6.3.	AIM-EIS	36
2.6.4.	OPA	38
2.6.5.	eLearning	40
2.6.6.	eDirectives	41
2.6.7.	mySPD	43
2.6.8.	Computer Aided Dispatch (CAD)	43
2.6.9.	Performance Mentoring (PMP)	45
2.6.10.	Admin eForms	45
2.6.11.	Collisions	46
2.6.12.	InCar Video (ICV)	47

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

2.6.13.	Digital Evidence Management (DEM)	47
2.6.14.	Usage of Force (UOF)	48
2.6.15.	Street Checks	50
3.	<i>Current State with IAPro</i>	53
3.1.	Background	53
3.2.	Introduction to IAPro and BlueTeam	53
3.3.	Overview of IAPro and BlueTeam Capabilities	53
3.3.1.	Early Intervention Capabilities	53
3.3.2.	Analytical and Data Mining Capabilities	54
3.3.3.	Reporting Capabilities	54
3.3.4.	Case Management Capabilities	55
3.3.5.	Security and Access Control Capabilities	55
3.3.6.	Customization Capabilities	55
3.3.7.	Integration Capabilities	55
3.3.8.	Other Capabilities	56
3.4.	Overview of How IAPro and BlueTeam Will Be Implemented at Seattle Police Department	56
3.5.	Perceived areas of Risks and Gaps	58
3.5.1.	Overall Perceived Gaps and Risks	58

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

Terms and Definitions

Abbreviation	Definition
APEX	Application Express
BI	Business Intelligence
BP	Business Process
BPEL	Business Process Execution Language
BPM	Business Process Management
CAD	Computer Aided Dispatching
CI	Crisis Intervention
DBMS	Database Management System
DOJ	Department of Justice
EIS	Early Intervention System
ETL	Extract, Transform, Load
GO	General Offense
HR	Human Resources
IT	Information Technology
ITS	Information Technology Section
KPI	Key Performance Indicator
LAN	Local Area Network
OPA	Office of Professional Accountability
PMS	Performance Management System
QA	Quality Assurance
RAD	Rapid Application Development
RMS	Record Management System
SQL	Structured Query Language
SPD	Seattle Police Department
SSO	Single Sign On
UAT	User Acceptance Testing
UOF	Use of Force
WAN	Wide Area Network

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

1. *Executive Summary*

1.1. Introduction

The United States and the City of Seattle have entered into a Settlement Agreement and Memorandum of Understanding with the Department of Justice with the goal of ensuring that police services are delivered to the people of Seattle in a manner that fully complies with the Constitution and laws of the United States, effectively ensures public and officer safety, and promotes public confidence in the Seattle Police Department and its officers. As part of the agreement, a Monitor was appointed by the federal court to assess compliance and report on the implementation of this agreement. A Monitoring Plan has been established which provides a schedule and a blueprint for compliance with the Settlement Agreement.

The Monitor has identified a number of deficiencies with the Seattle Police Department's (SPD) current IT systems that may hinder compliance with the Settlement Agreement. The agreement requires the Seattle Police Department to have a robust IT system that operationalizes core functions of the department, provides officer performance insights to managers which will allow them to actively supervise and monitor their officers, and to have a comprehensive reporting mechanism to evaluate and assess performance metrics and outcomes as an early intervention system. In order to comply with the requirements of the Settlement Agreement, the Monitor has asked SPD to develop a mature and comprehensive solution that fulfills all these goals. This information will allow supervisors and officers to carry out their day-to-day operations, effectively manage their staff by identifying potential issues and problems that can then be corrected and prevented through training, supervision, coaching and mentoring, and provide needed training and mentoring to prevent potential problems. This system will also provide the department and the Monitor with greater visibility into SPD's performance data that will facilitate the assessment of compliance with the Agreements.

For the Seattle Police Department, information, communications and technology are pivotal areas in the transformation of Police operations. As SPD moves forward with improving accountability both internally and with the citizens of Seattle, the following have been identified as desired outcomes:

- Improved professionalism by building awareness and clarifying expectancies
- Provide uniform and consistent standards across the department
- Provide high quality training and the ability to assess its effectiveness
- Develop objective performance expectancies and strong mentoring dynamics with all levels of the organization.

As such, the Department seeks to ensure alignment of its IT systems, operations and processes with current and future needs of the solution desired by the Monitor to be in compliance and meet the goals outlined. To this end, SPD collaborated with an external consultant to review, assess, evaluate and make recommendations for a solution to meet its goals. The Project Team has carried out a Current State Assessment of SPD's existing IT systems, processes, technologies and operations to bring about the gaps and associated risks to determine readiness and maturity towards the desired Future State solution.

1.2. Objective

This document contains details on the Current State assessed of SPD's IT Systems, Technologies and Processes from the perspective of implementing a BI solution. In order to provide a holistic 360-degree assessment, there are three major areas in which the assessment has been carried out. The first part of the assessment starts out with assessing the capabilities of SPD's IT Department relevant to supporting the BI system and the second part delves more into some of the specific processes and tools for the different systems, processes and operations within SPD. The third part evaluates IAPro as an interim

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

solution since IAPro has been selected by SPD as an interim solution. It should be noted however, that the assessment has been carried out with a specific purpose of determining readiness for the intended Future State solution desired by the Monitor and to provide a roadmap towards it rather than a generic assessment.

Note: The Current State assessment was carried out at a high level with the aim of highlighting major risks and gaps to deploy and support a solution. This should not be considered an IT audit as this was not in scope for this exercise.

1.3. Journey to Date

The Seattle Police Department has partnered with an external consultant to achieve the following objectives as a result of their engagement:

- Carry out a high-level assessment of SPD IT's capabilities to assess their overall readiness towards a roadmap of a Future State solution to meet the Monitor's Compliance needs of a Performance Management System (PMS)/Early Intervention System (EIS) solution
- Develop a Future State Roadmap for successful transition to the desired Business Intelligence (BI) system
- Leverage the carried out assessments to arrive at budgetary options for moving forward with the desired Future State Solution and help in Vendor selection and strategy
- Bring about perceived Gaps and Risks in the Current State that might hamper SPD's ability to roll out the desired Future State Solution
- Recommend capability roadmap and maturity models for Future State transition

The following diagram depicts the approach that has been taken as well as the journey to date to achieve the intended objectives as well as the major activities and milestones leading to the End State recommendations. The high-level assessment has been carried out using the DEADONS+I and PARTS framework that is described in detail in the next section.



Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

1.4. Methodology

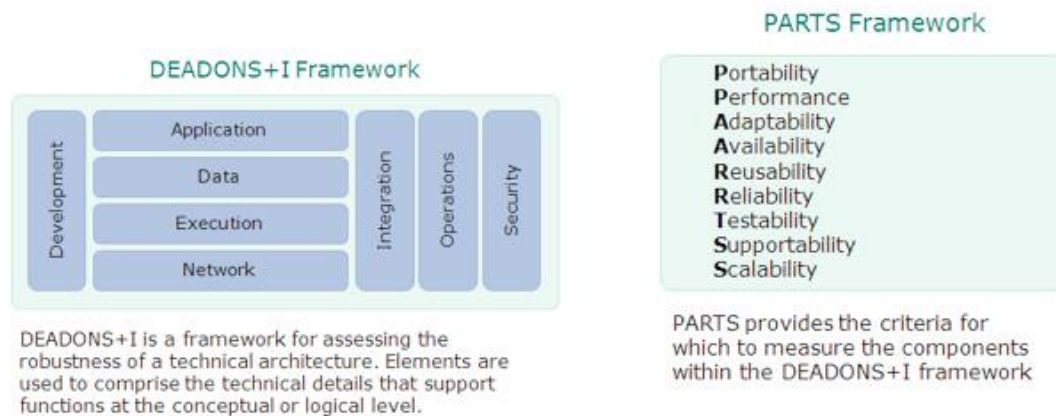
In order to expeditiously gather information on the current state, the Project Team executed the following major activities to obtain data about the current environment:

- Held a series of interviews with key functional departments and their business users that will be eventual users of the proposed system for a deep understanding of the desired functions of the proposed solution in the functional areas along with the dependencies, supporting data, supporting systems, processes and personnel
- Held a Briefing and Vision Casting sessions with internal and external SPD stakeholders to capture their vision and thoughts for the desired solution
- Held a series of interviews with IT stakeholders , various functional and technical leads within the IT organization for a deeper understanding of IT functions
- Applied the DEADONS+I and PARTS Framework to assess IT & system level capabilities and overall maturity levels
- Benchmarked applications to ascertain personnel productivity of supporting end-user applications

The Project Team assimilated the information gathered to render a maturity level for the IT capabilities and individual systems (e.g. business alignment and effectiveness of applications, etc.) across key dimensions of the DEADONS+I model: Development, Execution, Application, Data, Operations, Security, and Integration as exhibited in the graphic below. The DEADONS+I model has been used in conjunction with the PARTS framework to determine the maturity levels of various capabilities and systems as follows:

- The maturity scale is developed on an idealized basis, meaning that a Level 5 is the absolute best practice in the industry for that activity. Relatively few organizations make the investment to become Level 5 in all the areas, because it would be prohibitively expensive to do so without a commensurate return on investment
- Target states were determined using a combination of feedback from users' stated needs, capability towards achieving the goals of the desired solution and benchmarking with IT maturity models
- The Project Team applied a number of proven qualitative tools, quantitative tools and approaches to ensure a thorough analysis from a qualitative and quantitative perspective, where appropriate
 - Qualitative aspects: process maturity, user perceptions, alignment with best practices, etc.
 - Quantitative aspects: staffing, scheduling, availability, etc.
- The maturity scales used for these assessments use standard criteria that incorporate best practices. These maturity scales are industry-agnostic and place no value judgment on the IT services being delivered
- The maturity scale is developed on an idealized basis, meaning that a Level 5 is the absolute best practice in the industry for that activity. Relatively few organizations make the investment to become Level 5 in all the areas, as it would be prohibitively expensive to do so without a commensurate payback

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013



DEADONS+I is used to ensure the proper solution architecture artifacts are created to deliver the needed business capabilities:

- **Development:** The development architecture defines the software, tools, and facilities to support rapid prototyping and development of software within a structured and controlled environment
- **Execution:** The execution architecture defines a structured operating environment, hardware platforms, operating system software, and system services for executing application and business processes
- **Application:** The application architecture defines the system flows, interfaces and functional breakdown of the applications being developed. In addition, it provides a specification of the system components and interactions
- **Data:** The data architecture defines the tools, strategy, and services to address data definition and layout, data location and redundancy decisions, data update/refresh approach, data security, DBMS performance, and data backup and recovery of information assets
- **Operations:** The operations architecture consists of the combination of tools, support services, controls, and procedures required to manage the operation of the production environment and lab environments across the enterprise
- **Network:** The network architecture defines the strategy and components to provide reliable local area network (LAN) and wide area network (WAN) services, mobile access, and Internet access to support the implementation of client/server solutions
- **Security:** The security architecture defines the strategy, components, and processes to provide a secure platform for the enterprise. Application, system, and network security are all addressed
- **Integration:** The Integration Architecture defines and details the level to which systems can communicate and share data or business logic as well as ramp up to a middleware platform

We have used the following scale to rate the services as per the Capability Maturity Model. It is important to note that the model has two parameters. The rating for the Current State provides our assessment on the Current State of that particular aspect or Service whereas the Future State rating on the scale shows the maturity that needs to be achieved for the smooth rollout and operationalization of the End State proposed solutions.

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

Rating	Maturity Level	Definition	Code
1	Initial	<ul style="list-style-type: none"> • Demand for the capability is recognized by IT and the Business. • The starting point for use of a new or undocumented capability or process. (corrective measures to address immediate needs, ad hoc requests, individual heroics). 	
2	Repeatable	<ul style="list-style-type: none"> • Increased demand from multiple business functions. • Documented sufficiently such that repeating the same steps may be attempted. 	
3	Defined	<ul style="list-style-type: none"> • Capability recognized as necessary for improved business performance. • Processes for planning, design and development are defined and confirmed through published standards 	
4	Managed	<ul style="list-style-type: none"> • The organization recognizes the capability is required for competitive advantage • Capability is quantitatively managed in accordance with agreed-upon metrics. 	
5	Optimized	<ul style="list-style-type: none"> • Optimized and managed in the spirit of deliberate process optimization / improvement. • Service level agreements are in place and opportunities refinement and improvement are consistently reviewed. 	

1.5. Scope

The following aspects of IT have been considered in scope for the Current State Analysis:

Capability	Sub – Category	Description
Resources	Program Managers	Overall project management and governance
	Developers	Software developers
	Business Analysts	Analyze the existing or ideal organization and design of systems, including businesses, departments, and organizations, business models and their integration with technology
	Database Administrators	Installation, configuration, upgrade, administration, monitoring and maintenance of databases
	Business Process Definition/Owners	Work with Business and Functional Users to understand and document Business Processes using BPM standards like BPEL
	Sustainment Resources	Perform standard business processes
Tools & Technologies	Identity Management	Tools & technologies for providing role-based authentication

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

Capability	Sub – Category	Description
	Single Sign On	Tools & technologies for providing Single Sign On to various systems
	Integration	Tools, technologies & standards for middleware & integration
	Collaboration	Tools & technologies for providing collaboration & workflows
	Reporting	Tools & technologies for providing collaboration & workflows
	Data Services	Tools & technologies for providing data services
	Document Management	Tools & technologies for providing document management
	Mobile Applications	Tools & technologies for creating mobile & smart phone applications
	Portals & Web Services	Standards for portals and web services
	Functional Specifications	Assessment of functional analysis standards and processes
	Design & Development	Assessment of development standards and processes
Processes	Testing	Assessment of testing standards and processes
	Rollout	Assessment of rollout standards and processes
	Project Management	Assessment of program management processes and standards
	Configuration/Change/Release Management	Assessment of configuration management/change management/release management processes and standards
	Event Management	Assessment of event management processes and standards
	Governance	Assessment of governance processes and standards
Functional Areas within SPD	Security	Assessment of security processes and standards
	Use of Force	A Use of Force doctrine is employed by police forces, as well as officers on guard duty, to regulate the actions of police and guard
	Use of Force – Range Data	Assessment of Range application within context of Use of Force

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

Capability	Sub – Category	Description
	Use of Force – Canine Insights	Assessment of Canine usage within context of Use of Force
	Use of Force – Force Investigation Team	Assessment FIT team within context of Use of Force
	OPA (Office of Professional Accountability)	Assessment of OPA process
	Use of Force – officer Involved Shootings	Assessment of officer involved shootings within context of Use of Force
	PMS/EIS (Performance Management/Early Intervention System)	Assessment of PMS/EIS processes
	Pursuits	Assessments of police pursuits process
	Collisions	Assessments of police accidents
	Terry Stops	Assessments of Terry stops process
	Lawsuits	Assessment of named lawsuits as a part of the PMS/EIS process
	Training	Assessment of training process in PMS/EIS context

The following SPD Applications have been considered in scope for the Current State Analysis:

Application / Process	Description
PEDS	PEDS employee data system for requesting changes to employee data
AIM-EIS	Administrative Investigations Management Software
OPA	Office of Professional Accountability
eLearning	Online learning, training & certification tool used at SPD
eDirectives	Online system for issuing and ensuring compliance on directives and policy changes
Versadex RMS	Versadex Records Management System
mySPD	Personalized portal for role based access to targeted Services
Reporting Data Warehouse (RDW)	Centralized warehouse for CAD and RMS information
Computer Aided Dispatch (CAD)	Centralized call dispatching system
Performance Appraisal System (PAS)	Performance Appraisal System for performance management
Performance Mentoring (PMP)	Planned in-house PMS/EIS replacement for AIM
Admin eForms	System built to automate Use of Force, complaints and other OPA incident case workflows

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

Application / Process	Description
Versadex Versonnel	Centralized employee database, part of the Versaterm system
Collision	OPA incidents involving police accidents
InCar Video (ICV)	System for capturing dashboard camera video for evidence purposes
Digital Evidence Management (DEM)	Centralized warehouse of photos, audio and video evidence
Usage of Force (UOF)	Incidents involving an officer's Use of Force against a suspect
Street Checks (MRE)	System used to collect officer contacts with civilians

Considering that IAPro has been chosen as an interim solution, we have documented potential use of IAPro as a Current State solution in the following areas:

Capability	Sub – Category	Description
IAPro	Use of Force incidents	A Use of Force doctrine is employed by police forces, as well as soldiers on guard duty, to regulate the actions of police and guard. The tool will capture and report on UOF investigations process
	Office of Professional Accountability complaints	The Office of Professional Accountability is the office within the Seattle Police Department that receives and investigates complaints about police misconduct. The tool will capture details and report on OPA investigations
	Traffic – Pursuits and Collisions	Capture and report on officer involved pursuits and collisions
	Terry Stops	Capture and report on Terry Stops related detentions
	Early Intervention System (EIS)	Use early intervention and early warning to proactively measure, report, alert and take corrective actions
	Lawsuits	Capture and report on named lawsuits

1.6. Findings

As a result of the findings highlighted in the Current State assessment, a number of gaps and recommendations have been highlighted and documented in the Gaps Analysis document as well as summarized in the Future State Recommendations document. Gaps were found in several areas including:

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

Data Quality, Availability and Reliability: There are areas where data within the SPD is either inconsistent, inaccurate, out of date, or out of sync.

Data Management & Data Governance: There is a lack of data management and data governance practices within the department that results in inconsistencies across systems resulting in lack of data, inconsistent data, and inaccurate data.

Process Quality and Reliability: Key business processes are manual, paper-based processes that are not suited for use within the BI solution. As a result of data quality issues, reporting is also manual, difficult, and time consuming with limited value.

IT Governance: While some IT governance practices were noted, many could use improvements as they do not leverage tools or a robust enough process, such as project management, project portfolio management, change management, incident and problem management.

Resourcing: The BI solution would demand a large effort on the part of SPD and SPD IT. As it stands today, SPD IT is not able to support additional projects without current resourcing issues being resolved.

While there are gaps, it is important to note that there are areas where SPD IT is leveraging best practices, including:

- Leveraging emerging technologies such as cloud technologies to reduce data center footprint, operating and capital costs, increase resiliency for business applications as well as increasing time to market for new applications
- Albeit not enterprise grade applications, SPD has developed over 36 applications with a consistent look and feel that reduce training needs and addressed specific business problems.
- Improved training and directives management through the implementation of low cost open source platforms

Additional details on the findings can be found in the Gaps Analysis document.

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

2. *Current State IT Analysis*

2.1. Overview of SPD IT

The Seattle Police Department's mission is to work with the people of Seattle to secure a safe and just future for all by fighting crime, reducing fear and building community – one person, one community and one neighborhood at a time. The Seattle Police Department's Information Technology Section (ITS) works within the Field Support Bureau to support over 1,200 officers and 600 civilian employees of the Seattle Police Department execute on this mission. The focus of the Information Technology Section is to provide operational support to the IT environment, preserve security and to support new initiatives.

The SPD Information Technology Section is a team of thirty-seven staff distributed with the majority of staff aligned to three groups aligned to Services, Applications and Infrastructure. The Services group is focused on user-facing platform support such as desktop and mobile platform support. The Applications team provides SPD application and database support, middleware and web as well as development services. The Infrastructure team supports the operating environment for SPD, including network infrastructure, physical and virtual servers, their operating systems, as well as an enterprise storage environment with over one petabyte under management and an enterprise backup environment. In addition to the support groups, SPD IT also has two project managers who manage the program portfolio for both SPD IT initiatives as well as business initiatives.

The SPD IT organization supports a rather complex environment for its size and the complex web of city, state and federal regulations that it must operate in. With a staff of thirty-seven, the SPD IT organization supports a network infrastructure, 275 operating system instances across both physical and virtual servers, over 180 applications, 2,500 desktops and 300 mobile workstations, databases, middleware, web as well as applications core to the operation of the Seattle Police Department such as call dispatch systems, E911 and record management, a large storage environment to support increasing data demands such as In Car Video, and a backup system. In addition to this, SPD IT has developed a number of applications to support business needs within the SPD.

SPD IT provides services to all of the Seattle Police Department, which is spread over five precincts at over fourteen different locations and has specialty units ranging from SWAT, canine, bomb/arson, gang units, car, foot and bike patrols, to harbor patrols, motorcycles and mounted patrols. The SPD operates with a \$250 million dollar budget and took over 445,000 calls in 2012.

To serve their constituents, the SPD IT organization is aligned to several guiding principles. The first is to unify the department through IT systems that support consistent business processes. Secondly, is to build accountability and transparency. Finally, the SPD IT organization works to provide resilient systems to officers, civilian staff and consumers of police information by ensuring operational support, preserving security and supporting new business initiatives.

The Information Technology Section's approach to providing service is focused around collaborative decision-making, taking in to account Command direction, leveraging of a Technology Steering Committee, having sustainment standards and a Records Committee to review retention and risk, as well as project governance and an agreement on priorities.

Current drivers for the department included focused around supporting reforms of the Seattle Police Department and include implementing terms of the Settlement Agreement reached with the Department of Justice as well as supporting the SPD's 20/20 initiative to execute on twenty initiatives within twenty months. These initiatives range from addressing biased-policing, developing protocols to prevent low-level offenses from escalating, improve supervision with the creation of a Sergeant's

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

Academy to initiatives such as creating a culture of public service and improving transparency and accountability. Compliance and audits also drive SPD IT activities such as the CAU and VMDT audit.

SPD business priorities influence and direct SPD IT. In addition to its crime-fighting mission, SPD is focused on improving accountability, supporting citizen outreach, supporting city cooperative efforts, as well as moving to become a data driven organization, improving crime response, business management, criminal justice integration, internal communications and public disclosures.

In response to these business priorities, SPD IT has designed a future vision around several themes:

- To provide secure, universal access to actionable information via application- appropriate devices and mobile platforms
- To consolidate business processes and systems to increase consistency and efficiency by moving business processes to CAD/RMS wherever possible and building or buying solutions to address those processes which cannot be moved to CAD/RMS
- Unify business access to information and make sure the information is timely, relevant and reliable to drive data drive decision making, evidenced based policing and advanced analytics
- Provide easy access to data in order to support decision support systems
- Like any other organization, the Information Technology Section faces its own challenges. Some of these include:
 - Process maturity both internally and externally to SPD IT
 - Projects and new business initiatives have taken precedence over production support resulting in a backlog of technology issues in the form of deferred support and deferred replacement or upgrades to legacy systems
 - Explosive data growth from systems such as In-Car Video and DEMS have also pushed up the amount of data management and support SPD IT must perform, further pressuring staffing resources

Despite these challenges, over the last four years, a number of transformations have occurred within SPD IT. With the introduction of an internal cloud environment, SPD IT can bring up new servers in minutes compared to what used to take months with traditional methods. In addition, to this time-to-market efficiency, there are reduced costs associated with less space, less cooling and less power consumed by the environment as more applications are moved in to the internal cloud.

Furthermore, more than thirty-six applications have been put in to production with a common look and feel, allowing new systems to come online that are so familiar to users that additional training is not required. This strategy is allowing for progress in unifying police business processes and replacing bespoke unit-level processes with department-wide solutions. Purchasing and eDirectives are two such examples of these new department-wide solutions.

SPD IT has made progress in other areas as well such as unifying training and course information under eLearning, pushing new capabilities to mobile platforms, increasing use of social media as well as pushing IT-wide standards such as Single Sign On for applications.

Looking forward, SPD IT will continue on its strategies to unify business processes and increase access to useful, timely and relevant information for its constituents. Other future initiatives include a move to virtual desktops for mobile data terminals, consolidate their data center footprints by moving to the Next Generation Data Centers currently in planning, as well as exploiting external cloud offerings where appropriate and reduce technology footprints.

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

2.2. Notes on Current State Analysis

The following sections will be the heart of the Current State analysis with a focus on the technology, people, processes and systems used within SPD. Where applicable, the each component will be evaluated by the DEADONS+I/PARTS framework as well as rated on a maturity scale, as discussed in Section 1.3 of this document. It is important to note that this evaluation is not an IT audit; it is a high-level evaluation of IT technology, processes, people and capabilities as they relate to implementation of the end state solution and roadmap. It is also important to note that only the relevant parameters of the PARTS framework that apply to the assessment from the proposed Future State Solution perspective have been applied. In addition, the assessment covers the assessment of the Business Processes as well as the Technology Tools used to assess the process for a holistic assessment overall. The Process assessment aims to focus more areas such as availability or quality of Data (e.g. UOF) whereas the Technology Assessment is more around the Quality and Maturity of the Tools used.

2.3. Technology

The following sections will address assessment of the technology usage within SPD IT. The first aspect covered is usage of Single Sign On for Applications. For each area, there is a description of the Process or Tool followed by the DEADONS PARTS assessment.

2.3.1. *Single Sign On (SSO)*

2.3.1.1. Overview of Single Sign On

Single Sign On is especially important for SPD as many of the users of IT Systems at SPD are officers, supervisors, managers, and captains etc. who may not necessarily be technology users. Furthermore, they would be accessing the tools from a variety of form factors such as smartphones, tablets, in car consoles, workstations either from the field or from their desks. They may have limited attention span to the Applications from the field and may need a seamless experience to the applications from the limited time span that they may possess from their experiences in the field. Furthermore, the Single Sign On must be accompanied by role-based access from a security perspective. Single Sign On is also going to be a key aspect of the proposed Solution. In this section, we assess SPD's implementation of Single Sign On. The relevant PARTS Dimensions that have been used for the assessment are Availability, Reusability, Scalability and Supportability.

2.3.1.2. Assessment of Single Sign On at SPD

<u>DEADONS PARTS evaluated</u>		<u>Comments</u>
<u>AVAILABILITY</u>	<u>REUSABILITY</u>	<ul style="list-style-type: none"> SPD has made Single Sign On a priority and most of its tools are integrated with Single Sign On with appropriate role based access Oracle Access Manager is used as the standard for Single Sign On
<u>SCALABILITY</u>	<u>SUPPORTABILITY</u>	

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

<u>DEADONS PARTS evaluated</u>	<u>Comments</u>
	<ul style="list-style-type: none"> • The OAM Tool and Process is well scaled out and is highly available to most applications that need Single Sign On functionality with it. • The SSO Infrastructure is already being leveraged by a significant no. of Applications and can be extended to other Applications within the Department • From the Future State Solution perspective, the proposed Future State Custom Solution can be architected to leverage the SSO Capabilities based on OAM. • CAD and RMS have their own authentications and achieve Single Sign On Dynamic through LDAP • The OAM based solution is scalable as it works across most of the tools deployed at SPD • SPD has good skills on OAM and can support the tool for future requirements • Oracle Access Manager can be integrated with Active Directory

2.3.2. Data Management

2.3.2.1. Overview of Data Management

The desired future state system is proposed to be a Data rich system which will integrate and consolidate Data from multiple sources, both from manual inputs as well as from integrations from other internal and external Systems. It is therefore necessary to have strong, standardized and consistent processes around how Data is captured, validated, stored, defined and analyzed. Furthermore, these processes should be automated to the extent possible with the usage of technology systems and tools. This will ensure accuracy, reliability, consistency and completeness of Data at all times in the proposed Future State Solution. These processes are collectively being referred to as Data Management processes. Enclosed are some examples of best practices with Data Management processes: -

- Creation of an Information Architecture matching Information needs with information resources. A well-implemented architectural design structures information in an organization through specific formats, categories, and relationships. For example, a Use Of Force may involve usage of Weapons, Sprays or Body Parts as may be carried out through a Pursuit or in Interrogation. So as an Information Entity, it should be documented and defined across related entities and drill – downs. This will also ensure consistency in how the Information is stored across all Systems. As an example, if a Suspect's First Name and Last Name appear separately in one System and together in another System, it can get tough to correlate the same Suspect's identity across multiple Systems since there was no standardization in how the Suspect's Name is stored and referenced in the Organization.

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

- Creating Source System Mappings to have tracings identified to the Source Systems through which interrelated data will come together as one Database in the proposed Solution.
- Many reference data for analysis and reporting is stored in the respective Source Systems. Establishing a good Master Data Management practice through an Enterprise Master Data Tool will ensure that all the reference Information is contained in one place that be looked up as needed.
- Reducing the layers of Manual Input before Data is finally submitted into the System. For example, a manual transcription process taking Data from the Paper Forms and entering into the System should be avoided as it tends to generate information based on perception of the transcriber through an added layer of translation. Straight – Thru processing of Data from the source directly into the System to the extent possible with the necessary checks and balances and de – duplication would ensure a higher degree of reliability of the Information that is contained.
- A good Information System must not allow for any incomplete information to be stored. If incomplete Data is detected, the System should alert the respective End User to fill in the updates as part of a Workflow process. Furthermore, a good System should periodically run checks to scan for Data inconsistencies and flag the End Users for their pending actions. This will ensure clean and consistent Data at all times within the System.

Data Management or Information Management embodies a convergence of data quality, data management, data policies, business process management, and risk management surrounding the handling of data in an organization. Through data governance, organizations are looking to exercise positive control over the processes and methods used by their data stewards and data custodians to handle data. Strong Data Governance is going to be extremely important from the proposed Future State Solution perspective. The Future State Solution Warehouse is likely to be consolidated from multiple transactional Source Systems as well as Reference Master Data Systems. Therefore establishing Data Management, Data Governance and Master Data Management is going to be a very important part of the Solution. This section therefore looks at SPD IT's Data Management practices for the relevant Systems for the proposed BI Solution and summarizes the findings..

2.3.2.2. Key Findings with Data Management

<u>DEADONS PARTS evaluated</u>		<u>Comments</u>
<u>AVAILABILITY</u>	<u>REUSABILITY</u>	<ul style="list-style-type: none"> • SPD does not have good Data Management or Data Governance processes or solution in place • There is lack of an Enterprise - wide glossary and taxonomy that makes it hard to have a consistent definition of desired Insights, KPIs and source data. This was unearthed as one of the key issues in the establishment of Personas and their Information Needs. • Putting in place Data Management and Data Governance policies is going to be especially important from the point of view of an advanced analytics in the desired future state solution since there would be a need for common definition of data from source systems and inconsistencies in
	<u>RELIABILITY</u>	

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

<u>DEADONS PARTS evaluated</u>	<u>Comments</u>
	<p>data can be resolved. SPD has many source systems for different capabilities that need to be all integrated together for the purpose of providing advanced analytics for an Early Intervention System.</p> <ul style="list-style-type: none"> Looking at the needs of the desired End State System, the Processes most recommended to be put in place include the following: - <ul style="list-style-type: none"> Creating Information Taxonomy & Enterprise Data Glossary with Metadata Establishing Data Lineage Master Data Management Processes for Data Cleanliness, Quality, Consistency and Maintenance

2.3.3. Content & Document Management

2.3.3.1. Overview of Content Management

Effective content management is an important discipline that will be essential for the proposed future state solution. Effective content management practices entail a good repository for storing all documents and content related to key projects and initiatives. It should have good version control, good collaborative capabilities to work together on content, an effective way of creating and storing template based rich content, alerting and notification capabilities when the content undergoes a change. A content management tool and processes around it should automate the content lifecycle process.

InWeb is used as the native content management tool within SPD IT. SharePoint is only used by some developers. There is lack of SharePoint expertise within the organization. In general, document management takes place through file shares. An open source tool is used for code version control. A Citywide move to SharePoint is also being planned by the end of the year and expected to be operational by June of 2014, however, due to lack of resources, the SPD is unable to make this conversion.

In this section, InWeb's use has been evaluated.

<u>DEADONS PARTS evaluated</u>	<u>Comments</u>
<u>PERFORMANCE</u>	<p><u>STRENGTHS</u></p> <ul style="list-style-type: none"> Good, centralized way to store documents Good discipline maintained around storing of documents <p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> Not the City standard for document storage Have only some of the capabilities of an enterprise class portal

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

<u>DEADONS PARTS evaluated</u>	<u>Comments</u>
	<ul style="list-style-type: none"> – Lacks authentication and therefore advanced Security – HTML based and very simplistic – Looking at the needs of the Future End State Solution, it is highly recommended to leverage and build across the board expertise on a more sophisticated tool like SharePoint. Its usage is recommended for day – to – day Information and Content Management by both Business Users and Technical Users

2.3.4. Integration

Sonic is used as the Enterprise Bus Technology for distributed data between systems at SPD. Enclosed are key findings on Sonic as an Enterprise Middleware:

2.3.4.1. Overview of Sonic (Middleware Platform at SPD)

Progress SonicMQ is a fast, flexible, scalable e-business messaging server designed to simplify the development and integration of today's highly distributed enterprise applications and Internet-based business solutions. SonicMQ is a complete implementation of the Java Message Service v1.0.2, an API for accessing enterprise-messaging systems from Java programs.

To achieve an effective future state, a strong integration platform is needed to integrate and interoperate between the myriads of source systems and information messages that get exchanged across those. Therefore, the platform must be scalable, reliable, high performance message exchange system that can be extended to various source systems and be well supported by the staff at SPD. Enclosed is the assessment of use of SonicMQ at SPD.

2.3.4.2. Key findings with Sonic

<u>DEADONS PARTS evaluated</u>	<u>Comments</u>
<div>PERFORMANCE</div> <div>RELIABILITY</div>	<div>REUSABILITY</div> <div>SUPPORTABILITY</div>
	<p><u>STRENGTHS</u></p> <ul style="list-style-type: none"> • Sonic is an Enterprise wide Middleware Platform that scales well to meet the needs of the Enterprise. It operates in both a Scale – up mode as well as a Scale – out Mode. • SPD is leveraging Sonic in an effective way to meet its messaging needs. • Sonic can scale to meet the Enterprise wide needs of a Custom Solution as well as a Vendor Solution integrated with other Source Systems • SPD has good experience and skills with Sonic that can

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

<u>DEADONS PARTS evaluated</u>	<u>Comments</u>
	<p>be used for a Custom Solution</p> <ul style="list-style-type: none"> Sonic is fully compatible with the Java Platform used across the board at SPD as well as the AIM Platform

2.3.5. *Development Platform*

2.3.5.1. Overview of Apex (Development Platform at SPD)

Oracle Application Express (Oracle APEX, previously named Oracle HTML DB) is a software development environment that runs inside the Oracle database. APEX can be used to build complex web applications from scratch, using only a web browser.

As an application framework, it can be difficult to customize an application outside of a set of expectations about how an APEX application is supposed to operate. However, given that pages are built from customizable templates, anything that is possible to achieve with HTML, CSS and JavaScript is also theoretically possible to achieve with APEX, although it requires more work than using the built-in templates.

The current Development Platform is Apex 4.1. The new version of Apex is 4.2.3 that will be adopted. This Platform has a tool called Subversion for Source Code Control. Versaterm is an OS upwards Platform. Apex is very reliable and is leveraged on highly available servers and is highly scalable.

2.3.5.2. Analysis of Apex (Development Platform at SPD)

<u>DEADONS PARTS evaluated</u>	<u>Comments</u>
<div>DEVELOPMENT ENVIRONMENT</div>	<p><u>STRENGTHS</u></p> <ul style="list-style-type: none"> Web-based RAD Development Developers familiar with PL/SQL can use the same skill set when developing Apex applications without needing to know a Programming Language Make it easy to create mock-ups Easy to deploy (end user opens a URL to access an APEX application) Scalable (can be deployed to laptops, stand-alone servers, or Oracle RAC installations) Contains Server-side processing and validations Strong and supportive user community (especially Oracle APEX forum) Strong support for group development Apex applications can run on the free Oracle Express Edition (XE) database Individual components of an application can be retrieved or identified using SQL, facilitating

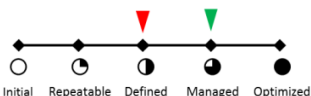
Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

<u>DEADONS PARTS evaluated</u>	<u>Comments</u>
	customized reports
	<p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> – Large installation size. The unzipped installation files for Apex 4.1 that includes 9 different languages for the "Application Builder" interface is 747 megabytes. The English-only version is 147 megabytes. Apex is installed on the database server; developers and users only need a web browser to build and use applications. – Primary keys can be at most two separate fields. However since version 4.1 Application Express supports the use of ROWID for updates, inserts and deletes as an alternative to specifying primary keys. – Pages in APEX can display at most 200 items and forms cannot handle more than 200 database items. Compare this to the Oracle Database where tables can have up to 1000 columns. Pages must be designed to work around this limitation, for example by using multiple pages, tabular forms, or Ajax for on-demand updates. – APEX applications are created using Oracle's own tools and only can be hosted in an Oracle database, making an implementer susceptible to vendor lock-in. – Few webhosts offer APEX on their hosting service package (most of them offer PHP + MySQL or ASP + MS SQL Server). Therefore, APEX applications are limited in their choice of webhosts. <p><u>RECOMMENDATIONS</u></p> <ul style="list-style-type: none"> – While Apex through its RAD may meet the need of quick and easy development of piecemeal Custom Applications, a more comprehensive Development Platform would be recommended for the Future State Solution considering the complexity involved – Additional developer resources to develop in and support a new, more robust application environment would be recommended – Training for the current developers in the new development environment

2.3.6. Overall Technology related findings

<u>OVERALL MATURITY LEVEL</u>	<u>Comments</u>
	<p><u>KEY FINDINGS</u></p> <ul style="list-style-type: none"> – Good expertise on the APEX/Oracle Platform – APEX used as key platform for all Custom Applications – Good expertise and choice of tool for the Enterprise Bus

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

OVERALL MATURITY LEVEL		Comments
<div> <div> Maturity Rating </div> <div> <div>Current</div> <div>Future</div> </div> </div> 		<p>technology</p> <ul style="list-style-type: none"> – Good expertise and usage of Single Sign On Technology and Processes across the board. <p><u>RECOMMENDATIONS</u></p> <ul style="list-style-type: none"> – Recommendation to create the Data Management and Governance processes as a pre – requisite to the Desired Future State Solution. – Recommendation to move to SharePoint for across the board usage for Collaboration, Document Management and Content Management for effective Information Management – Recommend adding appropriate staffing resources to support Sharepoint as well as other data management strategies.

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

2.4. Resources

The following sections assess the staff resourcing within SPD.

2.4.1.1. Overview of Resources at SPD

SPD IT is a team of thirty-seven staff distributed across three groups aligned to Services, Applications and Infrastructure. The Services group is focused on user-facing platform support such as desktop and mobile support. The Applications team provides SPD application and database support, middleware and web as well as development services.

The below table illustrates staff distribution across the SPD IT department:

Function	Number of staff
Management	4
Team Leads/Supervisors	3
Program/Project Managers	2
Admin	1
Desktop Support	5
E911 Support	2
PEO Support	1
Mobile Support	3
Database Administrator	3
Message Switch Developer	2
Application Support Engineers	4
E911-GIS Support	1
Network Engineer	2
Network Administrator	1
Network Infrastructure	1
Video Specialist	1

The total time that the resources spend on various activities is distributed as follows:

	HR	IT Governance	Management	Operations	Support	Administration	New Projects
Admin	4%	3%	9%	11%	3%	14%	57%
Application	1%	0%	1%	13%	16%	25%	44%
Desktop	0%	0%	3%	15%	41%	19%	22%
Infrastructure	1%	1%	4%	26%	20%	21%	28%

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

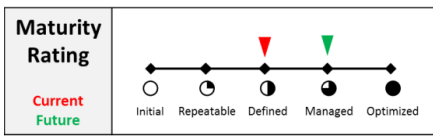
	HR	IT Governance	Management	Operations	Support	Administration	New Projects
SPD IT TOTAL	1%	1%	3%	16%	25%	21%	33%

- Overall, SPD IT is spending over a third of its time on projects and associated overhead, more than operational support, which is one of its primary duties
- Major projects tying up resources include Windows 7 upgrades and Access Database upgrades
- Unable to execute City-wide SharePoint migration due to resource constraints
- Only 1% of time spend on IT Governance activities

Other observations about resourcing include:

- The 2 Oracle DBAs support all Oracle Databases. A significant portion of their time is spent on databases of CAD and RMS as well as Apex development.
- There are 2 Project Managers managing all the projects
- The Developers are distributed as follows:
 - 2 Developers are focused on Sonic Bus Technology
 - 1 Developer is focused on Moodle Development
 - 4 Developers are focused on Apex Development
 - 1 Developer is focused on SQL Database Staff
 - 1 Developer is focused on Application Support for 3rd party tools
- There are only five engineers supporting the SPD network, 275 physical and virtual servers and over 1.2 PT of storage. Typical server to admin ratio is about 50:1 for the level of environment the SPD has, so there should be about 5 server admins just to support servers, 2 storage admins and 2 network admins.

2.4.2. Overall Resource related findings

OVERALL MATURITY LEVEL	Comments
	<p><u>KEY FINDINGS</u></p> <ul style="list-style-type: none"> – Our assessment found that SPD has good Quality of Technical Resources with great technical expertise and skills on standards and platforms. The interactions with the resources revealed good skill sets, thorough knowledge and understanding of Systems & Tools, creative – SPD IT is significantly understaffed with Resources

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

OVERALL MATURITY LEVEL	Comments
	<p>stretched across multiple assignments & projects. A lot of deficiencies in effective execution of Processes are as a result of over-utilized Resources</p> <ul style="list-style-type: none"> With 180+ projects underway as well as the SPD Support needed for the proposed Future State Solution, there is clearly a need for Resources with various Skill Sets. At a high level, about 10-20 additional Technology Resources would be recommended. These should be split across the following: - <ul style="list-style-type: none"> Program Managers Developers Business Analysts Database Administrators and Data Architects Security and Integration Architects Support engineers <p><u>RECOMMENDATIONS</u></p> <ul style="list-style-type: none"> Established need to hire more resources or leverage shared services model planned as a part of the Next Generation Data Center initiative Tools needed to on-board resources and have role based curriculums to take them to intended maturity levels

2.5. Processes

The following sections will address processes used within SPD IT.

2.5.1. Project Management

The Project Management processes and governance were examined as a part of this exercise, however, the project portfolio was not reviewed for relevancy of prioritization.

OVERALL MATURITY LEVEL	Key Findings
<p>Maturity Rating</p> <p>Current Future</p> <p>Initial Repeatable Defined Managed Optimized</p>	<ul style="list-style-type: none"> Excel Spreadsheet Templates are carried out for Project Management MS Project is used for Timeline / Dependencies SharePoint is used for some Projects There are 2 Project Managers that manage most of the Projects at SPD – IT The Project Managers have good Project Management Skills Small projects typically do not get project management nor follow the project management framework

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

OVERALL MATURITY LEVEL

Key Findings

RECOMMENDATIONS

- Need for a structured PMO Organization
- A more formalized project management framework should be adopted as not all projects have the same governance
- As IT resources are over-utilized, a review of projects to prioritize would be recommended
- Need for additional Project Managers if projects cannot be reduced
- Project Management needs to be integrated into overall Governance Process

2.5.2. Configuration Management/Change Management/Release Management/Event Management

OVERALL MATURITY LEVEL

Key Findings

STRENGTHS

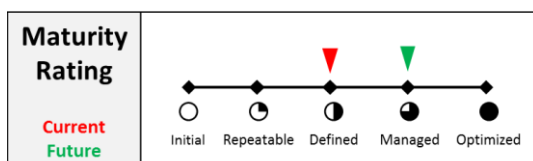
- Really Good Discipline around Change Management Processes
- Change Management is carried out through an E – Mail based process through a Change Management Log
- It's mostly manual or e – mail based
- The Change Management Log is captured in a Spreadsheet
- The Change has to be signed off by the Business Analyst

WEAKNESSES

- No Workflow Process associated with Change Management
- Difficult to trace status of specific change request at any given point in time
- Event Management is mostly Log Based

RECOMMENDATION

- A structured tool based process is recommended from the point of view of the proposed Future State Solution
- SPD should create Processes around Change, Configuration and Release Management and select a



Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

OVERALL MATURITY LEVEL

Key Findings

Tool best suited to meet their Requirements

2.5.3. IT Governance

The following observations were noted on IT governance:

- IT Governance is carried out through a Technology Steering Committee chaired by Chief Reid
- For new initiatives or to get initiatives on the priority list, a Project Charter is created. This is passed to Chief Reed from where it is passed to the Tech Steering Committee
- The Chain of Command Approval gets the initiative prioritized
- Basic project management, change control, asset management, problem and incident management processes observed

OVERALL MATURITY LEVEL

Key Findings

STRENGTHS

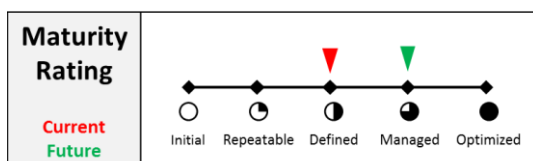
- There is some discipline around some processes. However, structured Processes are needed accompanied by the right Tools for most effective Governance
- Good interconnection between Technology and Business Users. Both are well supported by each other which helps in effective Governance through a de-centralized model

WEAKNESSES

- Basic governance processes in place
- Structured Tools based Governance Processes are needed in place. Currently the Governance may not be optimum primarily owing to lack of Resources
- No controls observed on governance processes

RECOMMENDATION

- As recommended earlier in the Document, the most important Governance Processes that are needed from the perspective of the Desired Future State Solution are the Data Governance Processes around Lineage, Quality, and Master Data, etc. These are recommended to be prioritized and staffed appropriately
- Look to implement IT governance best practices as



Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

OVERALL MATURITY LEVEL

Key Findings

provided in a widely used framework like ITIL or COBIT

2.5.4. *Development Standards*

The following sections will describe how SPD's IT development environment is organized.

2.5.4.1. SPD IT's Development Organization

SPD IT has a Development and Support Organization that focuses on building and supporting primarily APEX based Applications and Tools. Enclosed are some details on how the Developers are allocated:

- 2 Developers are assigned to Bus technologies as their core assignments
- 1 Developer is focused exclusively on Moodle
- 4 Developers are dedicated to Apex
- 1 Developer is assigned to SQL Database related activities
- 1 APEX Developer provides support for 3rd party Tool
- In addition, there is Tier 1 and Tier 2 support to provide 24/7 support.
- 2 Oracle Developers support all Oracle Databases for CAD/RMS/APEX
- Oracle Access Manager for Single Sign – On is a shared responsibility across the board

2.5.4.2. Key findings

OVERALL MATURITY LEVEL

Key Findings

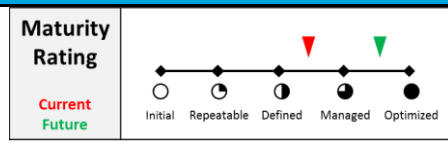
STRENGTHS

- Proficiently skilled Developers with good knowledge of their platforms
- Both Waterfall and Agile Models are followed for Development
- Typically for Projects, Project Charters and Business Workflows are created

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

OVERALL MATURITY LEVEL

Key Findings



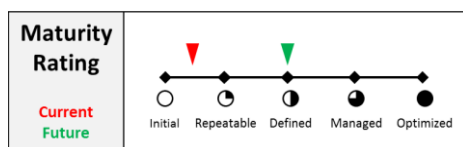
WEAKNESSES

- Consistent with the other areas, there is a shortage of Developers with more needed. The assessment found Developers doubling up as Testers
- There is not a True Development Environment at present
- Most Development is carried out in Production Environment
- A Cloned copy is made of the Production Environment
- The Development is carried out on the Cloned Copy
- Once live, the earlier Production Environment is deleted

2.5.5. Testing Standards

OVERALL MATURITY LEVEL

Key Findings



- No specific Testing Standards followed
- Developers double up as Testers

Recommendations

- Need to follow specific testing standards
- Need for testers to be hired
- Structured process needed for Unit, Functional, System Acceptance Testing

2.5.6. Security

SPD has strict requirements on security. Some of our findings are presented as follows:

OVERALL MATURITY LEVEL

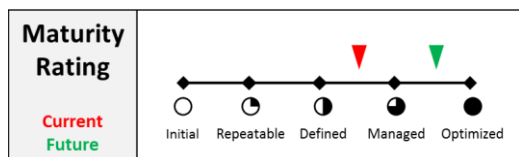
Key Findings

STRENGTHS

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

OVERALL MATURITY LEVEL

Key Findings



- Single Sign – On with secure Role Based access has been implemented as a priority for most Systems
- Laptop Hard Disk Drives are encrypted as appropriate
- Standard Certification Tools are used as Certs for Applications
- Documents are Password protected
- The Compliance Team is granted Read Access to everything
- Access Data is encrypted as part of the SEAJIS requirement

WEAKNESSES

- File Shares are not encrypted
- Duet Standards suggest implementing SQL Server 2008 with Encryption
- While there is role based security, incorrect HR data may weaken security measures

2.6. Systems

The following sections will address IT systems used within the SPD.

2.6.1. PEDS

2.6.1.1. Introduction to PEDS

PEDS is the Police Employee Data System. It contains details of the organizational reporting structure of SPD and is a custom application written by SPD that is a request system with associated workflow as well as a central repository for personnel data. The system is built in Oracle's rapid application development systems, Apex and is a wrapper for making updates to Versonnell, however, PEDS does not update Versonnell directly. Updates to Versonnell are made manually by hand, as direct updates to the Versonnell database are not supported by the vendor.

PEDS is primarily a request system that allows anyone within SPD to make requests such as rank & title changes; PEDS can be used for enhanced supervision to retrieve employee names, ranks & titles. It's the one – stop shop for all Employee Information. Every time a new Employee is hired, his details are updated to PEDS. PEDS stores an audit history and can be used for tracing purposes. PEDS' primary objective is to eliminate paper-based processes for changing employee details and to serve as a personnel data repository outside of Versonnell that can be leveraged by other SPD applications.

PEDS was put in place three years ago to replace an Excel spreadsheet based system that was in place. It was developed primarily as a request system since Versaterm does not allow direct updates to its database. Prior to PEDS, the Sustainment Group received Excel spreadsheet requests. There was no way to track request status and approvals that led to the introduction of PEDS.

PEDS provides a simple, user-friendly method of submitting information that groups forms by type of action. Within the form, utilize tools such as, drop down lists, auto-population of fields, enforcement of

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

business rules and mandatory fields. It allows the Department to begin expanding the collection of data in order to provide enhanced reporting needs and furthering the Department's goal of a centralized data repository. PEDS also allows Sustainment the ability to review and approve before manually entering the data into Versenel.

The way PEDS works is as follows. A request is made into PEDS. The Sustainment team receives and validates the request. Upon the approval and validation of the request, the Sustainment team will update Versenel.

PEDS has the following benefits:

- Repository data for personnel data outside of Versenel and provides a personnel data repository that SPD-developed applications can leverage
- Reduce or eliminate redundant personnel related information going into disparate databases
- Improve accuracy and timeliness of InfoView Employee assignment reports
- Emergency contact rosters will be more accurate and current
- Enhance existing special event and emergency operations by ensuring that the Operations Center has the most current, accurate information available when creating staffing plans
- Ensure that field supervisors have current and accurate specialty skill and equipment information for officers assigned to police events
- Maximize employee efficiency by eliminating manual entry
- Solves a record locking problem in Versenel
- Encourages increased updating of data due to ease of use
- Further the Department's current objective of "real time" employee tracking

PEDS stores the following fields of information:

- UID (Unique Identifier)
- Employee Name
- Rank & Title
- Employee Geography & Location
- Unit Assignment
- Emergency Contact Information

Examples of PEDS usage scenarios include:

- An officer's change of name changes also updates their exchange address
- Unit changes

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

- Title changes

PEDS provides a query interface and a wrapper to Versonnel. PEDS also stores a copy of personnel information and is leveraged by other SPD applications outside of Versaterm. PEDS is built on the APEX with an Oracle Database on Linux. PEDS has a web-based interface based on HTML/EJB. The APEX environment is hosted on Oracle Virtual Servers hosted on Oracle Hardware. Versonnel is hosted on a Linux operating system developed on 4J language with an Oracle database as the back end.

DEADONS PARTS EVALUATED	Comments
<u>PERFORMANCE</u>	<p><u>STRENGTHS</u></p> <ul style="list-style-type: none"> – PEDS is based on a strong technology platform and has no issues with performance, scalability – Does a good job in shielding End Users from the complexity of making updates and querying in Versonnel – Integrated with Single Sign On
<u>DATA</u>	<p><u>STRENGTHS</u></p> <ul style="list-style-type: none"> – PEDS is one repository for employee data leveraged by SPD applications – Every Officer is identified with a Unique Serial No. through which associations can be made to other Systems for Reporting <p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> – Personnel data in PEDS, Versonnel and EV5 l is not kept in sync nor is it checked for accuracy – Data reported to be inaccurate and not kept up to date
<u>REPORTING</u>	<ul style="list-style-type: none"> – Custom queries can be made to the PEDS Database through SQL queries – The queries can be made through the Sustainment Teams
<u>INTEGRATION</u>	<p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> – AIM has a hierarchy based on Roster File from PEDS extracts – The hierarchy from PEDS is updated into AIM every 4 – 6 months with the purpose of providing basic lookup and validation – However when the details of an OPA investigation are entered, the hierarchy from PEDS is uploaded into AIM and the AIM defaults are overridden. The AIM Hierarchy cannot be relied upon because of monthly updates in Roster file

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

<u>DEADONS PARTS EVALUATED</u>	<u>Comments</u>
--------------------------------	-----------------

SINGLE SIGN - ON

STRENGTHS

- PEDS is integrated with Active Directory through Single Sign On. Queries are made against Active Directory. Single Sign On is achieved through Oracle Access Manager.
- Sonic Integration can be achieved through loosely coupled Web Services through POST and GET calls.

2.6.2. AIM

2.6.2.1. Introduction to AIM

The Administrative Investigations Management system, AIM, provides agencies with a tool to collect, manage, track, analyze and report on a select range of data including Internal Affairs, Use of Force, Pursuits, Accidents, Awards, Time/Attendance and other data related to employee professionalism, performance and productivity. AIM is based on VB 6 and SQL Server 2000 hosted on a Windows Server 2000. It is hosted at SPD premises. AIM is a thick client tool with no web interface.

2.6.2.2. Analysis of AIM

<u>DEADONS PARTS EVALUATED</u>	<u>Comments</u>
--------------------------------	-----------------

DEVELOPMENT

WEAKNESSES

- There is currently no Development work that takes place on AIM
- Work is carried out with the Vendor through WebEx
- Application Queries are generated and data is exported as a result

STRENGTHS

- AIM is a repository of case data

DATA

WEAKNESSES

- AIM does not store all relevant data about cases and incidents, requiring additional manual lookups from paper files

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

<u>DEADONS PARTS EVALUATED</u>	<u>Comments</u>
<u>REPORTING</u>	<u>STRENGTHS</u> <ul style="list-style-type: none"> – AIM is a repository of case data – Application queries are generated and data is exported as a result – AIM is browser based and supports IE 8 or 8, 32 – bit versions integrated within Flash which makes for conducive Browser based report viewing
<u>INTEGRATION</u>	<u>WEAKNESSES</u> <ul style="list-style-type: none"> – AIM has a hierarchy based on Roster File from PEDS – The hierarchy from PEDS is updated into AIM every 4 – 6 months with the purpose of providing basic lookup and validation – However when the details of an OPA investigation are entered, the hierarchy from PEDS is uploaded into AIM and the AIM defaults are overridden. The AIM Hierarchy cannot be relied upon because of monthly updates in Roster File updating
<u>SINGLE SIGN - ON</u>	<u>WEAKNESSES</u> <ul style="list-style-type: none"> – AIM is not technically integrated with AD and SSO – AIM has its own User Management System with its own Authentication and Authorization – AIM has no integration with Oracle Access Manager – The hierarchy from PEDS is updated into AIM every 4 – 6 months with the purpose of providing basic lookup and validation – An Authorized Users List is handed to Business Users and is maintained by them

2.6.3. AIM-EIS

2.6.3.1. Introduction to AIM – EIS

An Early Intervention System (EIS) and Program has been developed for the purposes of identifying and supporting Department employees who demonstrate symptoms of job stress, training deficiencies, biased policing and/or personal problems that may affect job performance. The purpose of the Program is to identify employees exhibiting signs of stress, bias or unsatisfactory performance early on and intervene and provide support and counseling before it can affect the employees' performance or result in conduct that is contrary to the mission and fundamental values of the Department. The ultimate goal of the program is to support the employee's career development through counseling, training and correcting behaviors through early interventions. EIS has been defined as needing to happen on a weekly to monthly basis.

The following key specifications have been proposed for the PMS/EIS System:

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

- Should look at attendance, leaves, and balances etc.
- Should have timely information and analytics
- Should generate thresholds need for the following areas:
 - UOF
 - OPA
 - Collisions
 - Lawsuits
 - Pursuits
 - Accidents
 - Stops & Detentions
 - Citations/Collisions
- Should have flexible analytics
 - e.g. no. of people stopped in a specific precinct by a specific officer

2.6.3.2. Analysis of AIM – EIS

<u>DEADONS PARTS EVALUATED</u>	<u>Comments</u>
<div data-bbox="285 1397 601 1487"><u>PROCESS</u></div>	<p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> – At present, the EIS System is Manual, ideally it should be automated from HR Systems – EIS related Reports are sent to precinct, section captain in paper copies – From the time an incident happens to the time it is entered in EIS, it sits on the desk of paralegal; there is also a staffing gap here; there is a backlog usually on the Admin. Desk – Gap between the Data collected and entered for EIS – EIS should be automated from HR Systems but is not at present
<div data-bbox="285 1852 601 1942"><u>DATA</u></div>	<p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> – Paper based copies are forwarded down to Chain of Command – There are Silos of Data that need to be looked at which are not being looked at. There are huge volumes of indicators that are available and can provide EIS indicators but are not being looked at from an EIS perspective

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

<u>DEADONS PARTS EVALUATED</u>		<u>Comments</u>
		<ul style="list-style-type: none"> – When a lawsuit happens, there is a long process gap; till the time it is settled, it cannot be entered into the EIS System
		<u>STRENGTHS</u>
		<ul style="list-style-type: none"> – AIM provides a good repository of case files
		<u>WEAKNESSES</u>
		<ul style="list-style-type: none"> – Reports are generated manually. No way of periodic auto generation of reports based on thresholds. – Lack of timely information and analytics to Precinct Captains

REPORTING

2.6.4. OPA

2.6.4.1. Introduction to OPA

The Office of Professional Accountability is the office within the Seattle Police Department that receives and investigates complaints about police misconduct. OPA Cases are one of the most important triggers to an PMS/EIS System. There are about 2 OPA Cases that take place in a month. OPA is used at multiple levels by Chain of Command:

- OPA Group
- OPA Director
- EEO Sergeants
- Chain of Command

The OPA process kicks off once on a complaint has been issued. An intake interview is conducted and entered in AIM. Subsequent to that, the investigative process commences. OPA has key interdependencies with DEMS which is referred to as needed to view the evidence.

An OPA application was developed as a tool in APEX with strong analytical capabilities and was perceived to have the following benefits:

- Provide ability to do data entry of complaints by others outside of OPA
- Provide integrated workflow and time-bounded notifications
- Provide workflow for the appeals process
- Provide auto generation of communications as much as possible
- Provide data for mySPD and provide tracking of PDR – allowing scan of all case documents to be attached and then logged when requested.

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

The desired system was expected to have the following key success criteria:

- Should be transparent
- Should have more robust reporting
- Should provide ability to chain-of-command staff to enter, review, and finalize their portions of the workflow
- Provide OPA with integrated workflow to pass cases through internal chain-of-command in a time-constrained manner (mandated by the Settlement Agreement)
- Provide Legal & OPA ability to track a case through the appeals process
- Provide data for communications in the form of reports and memos as much as possible (barring constraints of Apex)
- Provide data for future project, mySPD that will improve communication with the affected employee and their chain-of-command
- Provide ability to attach scan of closed case and logging of PDR responses
- EEO has moved from OPA to HR creating the need to have OPAS available for data entry and case management for EEO cases.
- Legal has a need to provide data to OPAS for appeals and to be able to run reports out of the system – they will also need access to the completed case prior to the appeals process

2.6.4.2. Analysis of OPA System

<u>DEADONS PARTS EVALUATED</u>		<u>Comments</u>
<u>PERFORMANCE</u>	<u>STRENGTHS</u>	<ul style="list-style-type: none"> – The Solution was developed in the Apex Development Environment and tested for scalability, performance and availability – Excellent feedback was received during User and Functional Testing – The solution performed well to desired functionality
	<u>WEAKNESSES</u>	<ul style="list-style-type: none"> – The only perceived challenge was the integration of historic data residing since 2007
<u>DEVELOPMENT</u>	<u>STRENGTHS</u>	<ul style="list-style-type: none"> – The Solution was developed on Apex Development Standards and Best Practices from Oracle – The Development was completed in the stipulated time frame with few bugs – The User involvement was from the very beginning with User Feedback captured at every stage
	<u>WEAKNESSES</u>	<ul style="list-style-type: none"> - Reporting not available with APEX platform as-is - No analytics available

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

<u>DEADONS PARTS EVALUATED</u>	<u>Comments</u>
<p><u>ADAPTABILITY</u></p>	<p><u>STRENGTHS</u></p> <ul style="list-style-type: none"> – A good training plan was created to get Users trained and working on the new System <p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> – The biggest perceived challenges were getting populous buy – in and getting adopted to the new System

2.6.5. eLearning

2.6.5.1. Introduction to eLearning

eLearning is the system for officers to get certified and for officers to track training and certification of officers. The eLearning system tracks all internal training. It has extensive reporting capabilities and provides key insights into the following:

- Who's taken training
- Who needs to take training
- Training on what constitutes bias
- Training for stops and detentions etc.
- When training is due or overdue for an officer

The training has an evaluative component at the end as a test. The tool is based on the open source Moodle platform. There is a tool within Moodle to integrate people and groups. For example, the ICV course group would have sworn officers with Unit Numbers, Serial Numbers across the North Sector, Lincoln Squad. The objective is to associate the group with a course and sign the members within the group for the course.

The current eLearning system has been customized with additional custom modules and has been in production for the past 18 months. The core functionality offered by the System is 80% Out Of Box. The system is supported through a Virtual Server Linux Platform and developed on the LAMP Stack with a PHP based development on MySQL. For development and debugging, Moodle supports Firebug, a Firefox based plug-in for integrated debugging. The system is a thin client browser supported environment.

The system needs to be extended to field training officers that graduate out of the academy. The first year the officers are on probation and need to be observed on a daily basis. Multiple 30 – day

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

assessments need to take place as part of the field training system. Depending upon individual level, each individual person needs to have a separate list of field training requirements.

Due to architectural limitations within Moodle, the platform is unable to accommodate any training that needs re-certification or has an expiration such as qualifications. A separate tool will be needed to address this.

2.6.5.2. eLearning Assessment

<u>DEADONS PARTS EVALUATED</u>	<u>Comments</u>
<u>PERFORMANCE</u>	<p><u>STRENGTHS</u></p> <ul style="list-style-type: none"> – The solution performs well to desired functionality for training – It is used quite extensively for training and certification and a key tool for ensuring compliance with training for officers and Supervisors <p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> – Unable to accommodate qualifications
<u>DEVELOPMENT</u>	<p><u>STRENGTHS</u></p> <ul style="list-style-type: none"> – The Solution was developed customizing the Moodle Platform with about 80% of Out Of Box Moodle Functionality used – The Development was completed in the stipulated time frame with few bugs <p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> – Cannot be modified to accommodate qualifications training or any other training which requires periodic recertification
<u>INTEGRATION</u>	<p><u>STRENGTHS</u></p> <ul style="list-style-type: none"> – Integrated with Versaterm through upload of a Roster File – Integrated with Active Directory for Password Authentication <p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> – No mechanism or process for real time updates Roster File updates can have months lag at times – No integration with Single Sign – On/OAM – Lack of direct integration with Versaterm makes it tough for generation of PMS/EIS insights – Technical integration with Versaterm is achieved through SQL Queries

2.6.6. *eDirectives*

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

2.6.6.1. Introduction to eDirectives

eDirectives is a tool developed in APEX to automate the life cycle of publishing new directives , ensuring they are read and adhered to. Approximately four directives are issued in a business month and involve all circulars/memos associated. Upon reading the Directive, the officer has to undertake a test and pass the test. Clearance is based on answering all the questions. A Summary Report comes out giving details on who has taken the test and cleared. To ensure compliance, the officer has to read the directive and take the test associated with it. The Policy creation takes place through the Ideafield tool, which publishes into eDirectives.

eDirectives is an important tool from the PMS/EIS perspective to ensure officers are fully compliant with the latest directives. Some of the insights generated by the tool from a PMS/EIS perspective are presented below:

- When the directive was issued
- Who the e-mails were sent to
- Whether the associated officer opened the directive
- Whether the associated officer completed the course
- Whether the officer was certified on the directive
- When the officer read the directive
- Whether the officer understood the directive
- Was the directive followed when the officer got involved in an investigation

<u>PARTS DIMENSION</u>	<u>Comments</u>
<u>PERFORMANCE</u>	<u>STRENGTHS</u> <ul style="list-style-type: none"> – The solution performs well to desired functionality – It is used quite extensively for training and certification and a key tool for ensuring compliance with training for officers and Supervisors
<u>REPORTING</u>	<u>STRENGTHS</u> <ul style="list-style-type: none"> – The Solution was developed using Oracle APEX – The Development was completed in the stipulated time frame with few bugs <u>WEAKNESSES</u> <ul style="list-style-type: none"> – No Development weaknesses found
	<u>STRENGTHS</u> <ul style="list-style-type: none"> • Integrated with AD/SSO • Integrated with PEDS to generate insights such as:

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

<u>PARTS DIMENSION</u>	<u>Comments</u>
<u>INTEGRATION</u>	<ul style="list-style-type: none"> ○ Who was the Current Supervisor ○ Which ones were in Active Duty
	<u>WEAKNESSES</u> <ul style="list-style-type: none"> – No mechanism or process for real time updates Roster File updates can have months lag at times – No integration with Single Sign On/OAM – Lack of direct integration with Versaterm makes it tough for generation of PMS/EIS insights – Technical integration with Versaterm is achieved through SQL Queries – No integration with RDW – Data is all there in the Oracle DB but hard to Query

2.6.7. mySPD

2.6.7.1. Introduction to mySPD

The objective of mySPD was to provide a single point of information that allows an SPD employee to see all the information associated with them. Example Data includes:

- Training completed, training required to be completed, certifications and skills
- # of Use of Force, Collisions, or Pursuits reported
- Validate receipt of directives and orders
- Leave balances

The System was seen as a key contributor to Performance Management and EIS Capabilities by providing Role based personalized views and dashboards listing tasks, notifications, pending actions etc. against officers

- officer to see list of complaints against him in a personalized view
- Provide the same view of information for supervisors that staff can see
- Provide supervisors with the ability to see their staff's information from a single system
- Allows for consolidation of data across data sources from a single querying point

However, at the time of creation of this report, the System had not started being built and therefore, has not been analyzed.

2.6.8. Computer Aided Dispatch (CAD)

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

2.6.8.1. Introduction to CAD

CAD is a very core system from the PMS/EIS perspective but will continue to be used as an external Source System and has therefore not been evaluated.

The CAD system is a core system to police operations and has the following characteristics:

- CAD captures about 1000 events a day
- CAD System has two major facilities – in the West Precinct and Fire Alarm Services
- Components of the CAD System are used by the Justice Department
- CAD is mostly used as the main evidence system
- There are multiple areas where the evidence overall is located

2.6.8.2. CAD Platform

- CAD is a Versaterm based System
- The Versaterm System is a Linux based System based on VMWare Environment

2.6.8.3. CAD Interdependencies

- CAD is tightly integrated with the 9-1-1 System (please see details below)
- CAD works together with the Telephony System that is based on Positron/Viper
- CAD has strong interdependencies with the RMS System for Records Management
- CAD looks up the Map based location from the GIS System. The GIS System is a Mapping System which is maintained by SPU

2.6.8.4. 9-1-1 System

The 9-1-1 System has the following characteristics:

- The 911 calls go to the 911 System through the Phone Switches
- The NICE System records the 9-1-1 Calls. The Call is taken by a Call Center taker. Examples could include Police Fire calls or Emergency Response calls. The Call gets routed to the dispatcher.
- The Calls go to the ANI/ALI System which provides lookup of phone

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

- All the information located to the call is taken in the CAD System
- Based on the strong interdependencies between the CAD System and the RMS System, the records are transferred to the RMS System for Records Management purposes.

2.6.9. Performance Mentoring (PMP)

2.6.9.1. Introduction to PMP

PMP was intended as a replacement system for AIM as an Early Intervention System. The new PMP system was intended to automate data population, triggers and notification. Data was planned to feed into the PMP system from four existing systems. Triggers were designed to get tripped by data automatically feeding into the system. The system was designed to serve as the primary data entry interface for setting up custom thresholds that would trip a trigger when reached, and the associated action and tracking processes for that trigger, and setting up automatic notifications. The system allowed thresholds to be set for triggers to be activated by collecting and analyzing data for the following:

- Uses of Force (from Admin eForms)
- OPA complaints (from the new OPA system)
- Preventable collisions (from SECTOR)
- Lawsuits with named employee

The PMP System was perceived to have the following benefits:

- Reduced data entry effort and potential for transcription errors
- Integrated data flows between Admin eForms, OPA and PMP systems – integrated reporting of data
- Ability to set multiple thresholds for a single trigger category
- Automatic notifications that trigger thresholds have been reached and that action needs to be taken within a particular time frame

However, since PMP was not rolled out as a System, it has not been assessed.

2.6.10. Admin eForms

2.6.10.1. Introduction to Admin eForms

Admin eForms was developed as a tool to automate the UOF workflow and replace the manual paper-based process to capture UOF details. The tool was created to accomplish the following objectives:

- Provide electronic data entry, storage, management and access to admin packets

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

- Provide electronic workflow and approval process
- Identify and address data collection needs for querying

The tool was intended to automate the end-to-end processes involving Use of Force and be used for both the UOF incident details as well as the results of UOF and OPA investigations. It was intended to accomplish the following benefits:

- Provide electronic tracking of progress in workflow process
- Allow and track multiple users viewing, editing and moving (approving/rejecting) an admin packet through the workflow
- Provide log of an admin packet after workflow is complete
- Ability to query and analyse the data collected

The scope of this solution entailed creation of electronic data capture for the administrative forms involving Use of Force, Traffic Collision and Pursuits. It included the workflow process for each of these types of forms and was integrated with Active Directory to pull user login information and allow actions taken to be tracked. It provided notification for users at the different workflow levels when they were currently responsible for completing an action in the workflow. The solution was achieved in the following phases:

Phase I: Automating Use of Force (UOF) Packets – This phase included implementing electronic data submission forms, developing workflow processes and developing routing/tracking of UOF packets. It enabled UOF packets to be completed more efficiently and increased the visibility of UOF documentation. This made the workflow and routing processes more visible and thus more transparently reportable.

Phase II: Automating Pursuit and Collision Reporting – This phase includes implementing similar functionality as Phase I for documenting officer-involved pursuits and collisions.

It should be noted that Admin eForms has not been deployed and thus is not being assessed. Admin eForms was not deployed as it had lacked reporting functions and also was based on a business process that would significantly change due to the Settlement Agreement.

2.6.11. Collisions

2.6.11.1. Introduction to Collisions

Whenever an officer gets involved in a Collision, the details are stored in the Collision System. Collisions and Pursuits are captured as a manual process through paper based forms. These are then manually entered into AIM. The Data is then submitted by SPD into the centralized State system.

2.6.11.2. Interdependencies associated with Collisions

Collision data has strong associations with AIM EIS. All data related to Collisions, Pursuits and Citations is entered in AIM for Early Intervention purposes.

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

2.6.12. InCar Video (ICV)

2.6.12.1. Introduction to InCar Video

InCar Video is a repository tool used to archive video captured from dashboard cameras mounted inside police cruisers.

2.6.12.2. InCar Video Data Capture Process

The InCar Video Data capture process starts with the camera capturing an event and saving it. The save usually entails save from Start Time → End Time. The cameras are dashboard cameras mounted inside police cars to document activity. The System stores not just the videos but also the Data & Information associated with them as Metadata

2.6.12.3. Interdependencies associated with InCar Video

ICV is a standalone system, however, videos in ICV may be referenced by a case information from CAD or records in RMS (Records Management System).

2.6.13. Digital Evidence Management (DEM)

2.6.13.1. Introduction to Digital Evidence Management

DEMS is a repository tool for storing all types of digital evidence gathered during various types of interactions. It is referenced for tracking all evidence associated with a case. DEMs stores photos, audio recordings and video. These media files are stored in a proprietary format within a Microsoft SQL Server. The tool supports some reporting functionality, however, it is not used today. The tool has a lot of Human Intervention associated with Workflows and Approvals. DEMS is a third party tool supported by the vendor.

2.6.13.2. Interdependencies associated with Digital Evidence Management

DEMs have strong interdependencies with RMS (Records Management System). Information about all digital evidence is stored in RMS and RMS is used as a reference lookup to locate the evidence files for a particular case. The evidence files are stored in DEMs and retrieved from DEMs

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

2.6.14. Usage of Force (UOF)

2.6.14.1. Introduction to Use of Force

Use of Force is currently carried out through a paper based forms workflow system. Once the paper-based workflow is completed, the results are entered in to AIM. The information in AIM is used as a repository or catalog for Use of Force cases. Use of Force covers injury to officers as well as injury to People

2.6.14.2. Use of Force Data Capture Process

The details of Use of Force incidents are captured as a manual process through paper based forms. The embedded process diagram captures the detailed process for Use of Force. Every incident is captured as Type I, Type II or Type III Force. The details are entered first by the officer and then subsequently by a witness, his supervisor as well as an independent supervisor. A separate form is filled out for each civilian witness. The Supervisors get involved in Type II and Type III types of force usage. The UOF details entered go through a chain of reviews as specified in the workflow. The resulting XML document is converted into a Cube. Information from the Cube is written by the records staff into the RMS Database. Every Street Check incident that is entered is identified through a Street Check No. as a Unique Identifier. The details from the paper based forms are uploaded into AIM which is used as a Catalog or Use of Force.

2.6.14.3. Interdependencies for Use of Force

UOF has many associated interdependencies with other functional areas for EIS and Performance Management insights and reporting. Some of these are listed below:

- Associations with weapons data to ascertain weapons' usage during UOF incidents
- Association with Range data and eLearning data to determine certifications of officers to use specific weapons as well as handle specific type of situations involving Use of Force
- Association with Investigation data from officer Involved Shootings as well as Force Investigation Teams
- Association of UOF data with outcomes such as:
 - Injuries to suspects
 - Medical treatments received
 - Overnight stays at clinical care centers
- UOF associations with OPA complaints and investigations
- Associations with eDirectives data to determine whether issues directives were read and applied while UOF incidents

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

- Associations with collisions data to ascertain Use of Force in pursuits and collisions scenarios

2.6.14.4. Analysis of Use of Force

<u>DEADONS PARTS EVALUATED</u>	<u>Comments</u>
<u>AVAILABILITY (of DATA)</u>	<p><u>STRENGTHS</u></p> <ul style="list-style-type: none"> – The data capture forms are comprehensive and capture every detail entailed in a UOF incident – The forms are filled out by the officers as well as the supervisors – Every incident has officer Serial No. which can be correlated to PEDS database for linking purposes <p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> – Data is available but resides in physical form making it difficult to get insights as needed – Paper copies are kept locked up which makes it difficult to search them – Paper based forms carry historic data since 2007
<u>MATURITY (of PROCESS)</u>	<p><u>STRENGTHS</u></p> <ul style="list-style-type: none"> – Comprehensive workflow process for different types of UOF incidents <p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> – The entire process is a manual and paper based process – The process is time consuming – Since there are multiple packets of forms for every UOF incident, they move around physically making it difficult to keep track. Many times the packets reside on desks for long periods of time. – Difficult to track where the packets of paper might be located at any given point in time. – Difficult to track status of UOF process or investigation at any given point in time
<u>REPORTING</u>	<p><u>STRENGTHS</u></p> <ul style="list-style-type: none"> – Availability of the right data (though in paper form) for deep insights related to PMS/EIS functionality <p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> – Difficult to do any detailed trend analysis due to data residing in physical form
<u>INTEGRATION</u>	<p><u>STRENGTHS</u></p> <ul style="list-style-type: none"> – officer Serial No. is available along with the Incident # for every Incident making it possible to get officer details connecting with PEDS <p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> – No Integration with Active Directory or Single Sign On – No Integration with PEDS

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

2.6.15. *Street Checks*

2.6.15.1. Introduction to Street Checks

Street Checks is a process in the Versaterm suite. The key difference between a Street Check and Terry Stop is that a Street Check is classified as a Terry Stop when an officer proactively investigates and detains people from a Street Check. At that point, it is no longer a Street Check and is classified as a Terry Stop. As Terry Stops can be very subjective in nature, they are not currently recorded in the Street Checks process.

A Street Check is entered through the MRE (Mobile Report Entry) application. Information is entered as a free-form text descriptions and narratives with many fields available to report.

2.6.15.2. Street Checks Data Capture Process

The Street Check entry process is initiated when an officer files a report online. The online report is a manual process requiring manual validation. Every action performed by the officer has to be recorded. The Information has to be entered from mobile devices on bikes through the Mobile Report Editor Tool from Versaterm. Information can also be entered through the SmartPhone through a form that is consistent with the XML Format. The resulting XML document is converted into a Cube. Information from the Cube is written by the records staff into the RMS Database. Every Street Check incident that is entered is identified through a Street Check No. as a Unique Identifier.

Once a report is done in MRE, it is submitted and then reviewed by the supervisor. The supervisor may approve or may ask for more information. Once approved, the report goes through a QA process ("transcribed") to make sure its National Incident-Based Reporting System (NIBRS) compliant, needs additional info, supplemental reports, etc. Once done, the report is moved in to RMS system where it is stored.

2.6.15.3. Analysis of Street Checks

DEADONS PARTS EVALUATED	Comments
<div> <u>AVAILABILITY (of DATA)</u> </div>	<p><u>STRENGTHS</u></p> <ul style="list-style-type: none"> Provides a way to shield Business Users from making changes to RMS directly <p><u>WEAKNESSES</u></p> <ul style="list-style-type: none"> Most data is based on officers perceptions Data can be incomplete from a variety of reasons such as the person stopped did not give info, the officer could not ask the information, or the data may be kept out of the report as it may be sensitive in nature and could endanger the victim of a crime

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

<u>DEADONS PARTS EVALUATED</u>		<u>Comments</u>
		<p>(due to data disclosure requirements, there is a possibility the suspect can get victim data and go after them, etc.). What is entered in as purely up to the officer</p> <ul style="list-style-type: none"> There are hundreds of fields in the MRE application, most are hardly used. No fields are mandatory and data entered in is as the discretion of the officer, what s/he observed, etc.
<u>MATURITY (of PROCESS)</u>	<u>STRENGTHS</u>	–
	<u>WEAKNESSES</u>	<ul style="list-style-type: none"> SPD expect changes to the Street checks/GO processes, especially from DOJ agreement SPD team indicates that supplying the fields from MRE is not really possible With a General Offense report with an arrest, supervisor must screen suspect and approve, as well as submit a report. This is the arrest screening process and is manual. MRE has no rules on what the officer has to enter, and discretion is up to the officer depending on the circumstances (i.e. does the victim need protection, data disclosure concerns, etc.) A multitude of fields and a lot of information is collected on paper before it is entered in the MRE Application; as a result sometimes the info. in MRE is incomplete
<u>REPORTING</u>	<u>STRENGTHS</u>	<ul style="list-style-type: none"> Provides a way to shield Business Users from making changes to Versonnel directly
	<u>WEAKNESSES</u>	<ul style="list-style-type: none"> Difficult to do any detailed trend analysis due to the variance in data completeness. There are set fields, but data completeness of those fields vary greatly from record to record. Much of the report is also narrative which is not useful for reporting purposes.
<u>INTEGRATION</u>	<u>STRENGTHS</u>	<ul style="list-style-type: none"> officer Serial No. is available along with the Case # for every Incident making it possible to get officer details connecting with Versonnel MRE is integrated with Versonnel
	<u>WEAKNESSES</u>	<ul style="list-style-type: none"> No Integration with Active Directory or Single Sign – On No Integration with PEDS
<u>PERFORMANCE (of APPLICATION)</u>	<u>STRENGTHS</u>	–
	<u>WEAKNESSES</u>	<ul style="list-style-type: none"> Versaterm Application lacks referential integrity All Business Rules have to be written in 4J

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

3. *Current State with IAPro*

3.1. Background

The Seattle Police Department has decided to implement IAPro to automate some of the core functions of the Department and be compliant with the solution desired by the Monitor. This section of the document provides insights on how IAPro is intended to be used at SPD.

NOTE: It is important to be aware that there is limited information available at this point on the functional and technical specifications of IAPro. Therefore, based on the high-level understanding of the tool, many assumptions have been made regarding its capabilities. In addition, as the tool has not yet been rolled out, assumptions have also been made about how it will be operational on a day-to-day basis. The overall objective of documenting Current State with IAPro is to perceive foreseeable benefits and risks that might be associated with usage of the tool and its evaluation as a long-term solution.

3.2. Introduction to IAPro and BlueTeam

IAPro is an off the shelf early intervention system solution which provides support to OPA/Internal Affairs processes and is used by a number of police agencies across the United States and internationally. IAPro can manage OPA incidents including Use of Force, OPA complaints, pursuits, collisions. There is some capacity to add additional incident types. There are workflow abilities that allow cases within IAPro to have supervisory and command staff to review cases, make comments and approve cases once completed.

In addition to case management features, IAPro has built-in analytics, reporting, ad-hoc reporting and proactive notifications, giving the means to analyze and detect areas of concern in officer performance early.

IAPro is accompanied by a front-end companion package called BlueTeam. BlueTeam is for use by officers and their supervisors while IAPro is targeted for OPA incident cases. BlueTeam allows officers and supervisors to enter and manage incidents. A simple web-based interface is used to enter incidents including Use of Force, complaints, collisions and pursuits as well as other incident types. Incidents can be entered and then be routed through a review and approval workflow with Chain of Command.

IAPro and Blue Team were created by CI Technologies, who is the sole vendor for the product as well as the sole source of support. CI Technologies claims to have over 500 clients using IAPro around the world.

3.3. Overview of IAPro and BlueTeam Capabilities

3.3.1. *Early Intervention Capabilities*

The following PMS/EIS capabilities are noted:

- Alerting is based on pre-set thresholds. IAPro has seven different options for setting thresholds including:

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

- Basic incident type – based on number of incidents within a specific time period
- Advanced incident type – based on number of incidents over a specific time period but also factors in employees assignment to create a weighted score
- Overall – an aggregate of all incidents over a specific time period
- Monitored – any employee can be set to be monitored with this threshold; an alert would be created on any incident occurring
- Scoring-based model – threshold is triggered based on a percentile-based scoring model
- Supervisory – threshold based on supervisory role; allows for monitoring of incidents under specific supervisors once a set threshold is broken for staff linked to the supervisor
- Organization – threshold set based on organization
- Special alerts for officers of concern: An employee can be put on in a “monitored” state and alerts triggered upon any incident occurring

3.3.2. *Analytical and Data Mining Capabilities*

IApro’s analytical features come in the form of an inventory of pre-defined reports, a method to perform ad-hoc reporting as well as a Blue Team’s dashboard interface.

IApro supports the following types of analysis:

- Atypical performance identification – Groups employees and organizational units by selected incident types over a defined time period so that out-of-standard performance can be identified using ranking and top percentile analysis
- Peer group analysis – employees with performance issues can be compared with their peers
- Organizational analysis with headcount factoring – taking into account the size of the organizational units included in the analysis
- Trending analysis – over select time periods
- Drill-down analysis – Enables the further analysis by identifying the assigned employees with the most frequent performance issue

Blue Team’s dashboard function will highlight out-of-standard performance with a simple traffic light interface that allows the user to drill down to a specific employee.

3.3.3. *Reporting Capabilities*

A wide range of reports and charts are available. Features include:

- Over 120 pre-defined reports available
- Configurable charts
- Export of data to Microsoft Excel for further analysis

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

- Ad hoc query builder features allow the customer to create and save formats based on any combination of fields
- Supports secure access using third party reporting tools including:
 - Microsoft Access
 - Crystal Reports
 - SQL Server Reporting Services

3.3.4. Case Management Capabilities

Case management features included in IAPro and BlueTeam include:

- Case routing and case assignment capabilities and ability to add comments and instructions
- File attachments of documents to cases of various file types
- Built-in quality assurance to ensure data completeness
- Hierarchical case management interface allows for drilling down in to case details
- Security and access control over incident cases to allow only those with proper access to view or update cases
- Reminder function to help ensure cases move along the workflow in a timely manner
- Automatically produce due-dates for submission based on policy configured

3.3.5. Security and Access Control Capabilities

Security and access control capabilities included in IAPro and BlueTeam include:

- Role-base, hierarchical access control to segregate information only to those who should have access
- Access allowed on users role and users' assigned unit
- 26 controls currently offered to give a fine degree of access control within the application
- Access control on workflow queues
- Usage logs track user activity within the system including client details
- Password can be stored in an encrypted format

3.3.6. Customization Capabilities

IAPro has the ability to configure user definable fields. These include:

- Up to six organizational levels that can be defined such as district, squad, precinct, bureau, troop, etc.
- Up to two officer identifier fields as unique officer identifiers; these are in addition to badge number and unique officer number
- Pop-up list values can be customized by authorized users
- Automatic assignment of case IDs according to a customizable format which can be configured by the system administrator.

3.3.7. Integration Capabilities

IAPro has the following data integration capabilities:

- As a part of the initial deployment, a one-time conversion of legacy PMS/EIS application data is available

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

- Integration with HR data such as employee/officer data, attendance data and roster information is possible
- A limited number of external systems can feed in to IAPro such as case data

3.3.8. Other Capabilities

IAPro has the following other capabilities:

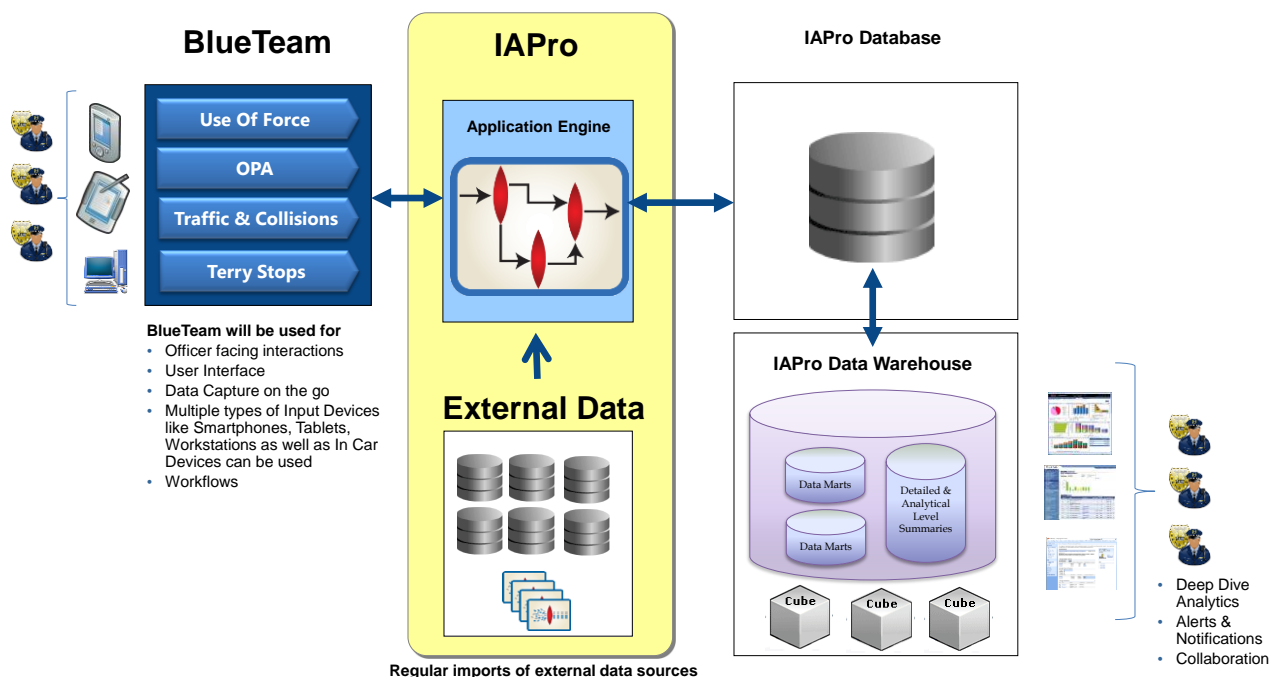
- BlueTeam supports data entry and queue management from a web browser
- BlueTeam includes routing of incidents via the Chain of Command with review and approval functions
- BlueTeam include features that integrate with internal e-mail systems so that supervisors are notified of new incidents that have been routed to them for review and approval
- Early intervention features that include alert override based on involved officer assignment, Use of Force alerts, allegation alerts, and supervisory alerts, organizational component alert and peer-group analysis
- Microsoft Word template integration
- A number of files of various types such as audio, photos, Microsoft documents, Acrobat, etc.
- Simple export of most reports' and early intervention interfaces' data directly to Microsoft Excel
- BlueTeam includes clickable body diagram for capture of force contact points and injuries
- Supports the following password security features:
 - A password minimum length can be configured
 - Passwords are stored encrypted in the database
 - Specify passwords contains one or more lower case character
 - Specify passwords contains one or more upper case character
 - Specify passwords contains one or more numeric character
 - Specify passwords contains one or more special non-alphanumeric character
 - Password re-use detection and limit so that a previously used-password cannot be re-used
 - User accounts are locked out after a specified number of unsuccessful logon attempts
- Able to integrate LDAP/Active Directory systems
- Supports both Microsoft SQL and Oracle databases

3.4. Overview of How IAPro and BlueTeam Will Be Implemented at Seattle Police Department

As IAPro has not yet been deployed within SPD, the following information is based on a number of assumptions gathered from the SPD team on anticipated use of IAPro. This is subject to change as SPD increases its understanding of IAPro, its features and gaps, how it will change their business processes and how it will integrate with other systems within the SPD.

The following diagram depicts the anticipated use of IAPro within the SPD:

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013



IAPro is intended to be used at SPD for the key areas of priority for SPD. These have been identified as:

- Use of Force
- Office of Professional Accountability
- PMS/EIS
- Traffic & Collisions – this includes Pursuits, Citations and Collisions
- Terry Stops

As mentioned earlier in the document, BlueTeam is the front-end companion of IAPro. This will be used in the field by officers on a day-to-day basis to enter details of policing activities. Details will be entered on various types of incidents by the officers and supervisors as deemed necessary based on the type of event. As the client is web-based, information can be entered from multiple types of form factors like smartphones, tablets, workstations and in car consoles. Suitability for these devices for use by SPD has yet to be determined.

IAPro does not have the ability to customize its business processes and workflows. As a result, the SPD has acknowledged this limitation and will adopt the business processes and workflows contained within IAPro.

A number of data sources such as HR data and case data from Versaterm is anticipated to be imported regularly in to IAPro. During the implementation phase, a IAPro engineers will work with the SPD to set up these regular import jobs which will be automated to execute on a regular basis, likely nightly.

Historical data on Use of Force, OPA complaints, pursuits and collisions held in AIM will be imported in to IAPro during the implementation phase. This will be a one-time event and it would be assumed that AIM will be decommissioned following the implementation of IAPro.

The disposition of information on paper records has not yet been determined. These could be left as-is, or SPD could have the documents transcribed in to a digital format then uploaded in to IAPro. As this would take considerable time and expense, it should be considered in depth during the design phase of the project.

Seattle Police Department Business Intelligence System	Version: Final
Current State	Date: 12/6/2013

3.5. Perceived areas of Risks and Gaps

3.5.1. *Overall Perceived Gaps and Risks*

While Iapro seems to be a comprehensive solution, it does not address all of the requirements set forth by the Monitor. The following areas have been perceived as possible issues with the use of Iapro:

- Gaps
 - There is lack of clarity on whether it handles intervention management
 - Import and integration with external sources is limited to the following data sets:
 - Human resources
 - Limited incident cases
 - Arrests/Booking
 - Sick leave/attendance
 - Discretionary charges
 - Missing data sources include:
 - Training
 - Qualifications
 - Missed court attendance
 - Commendations & awards
 - Policy/Directives
 - Threshold required by SPD (“smart thresholds” which factor in assignment, role and unit in to threshold) not available; however, there is a similar threshold which takes in to account assignment
 - No ability to customize the application workflows and business processes to fit SPD needs
 - No ability to customize the dashboard feature to provide other views of information
 - The Monitor stated that Iapro was an interim step, not a final solution
- Risks
 - Likely not to cover all requirements from the Monitor as not all themes addressed in Iapro
 - Vendor requires access to SPD systems to do integration and implementation

